Dc3 Digital Forensics Challenge

302 – SKYPE Communications Logs

Team Information	
Team Name:	@ls0 - r@n
Results Email:	[redacted]
Examination Time Frame:	to

Instructions

Description: Examiners must develop and document a methodology used to parse SKYPE communication logs from the communication/program files in the **302_SKYPE_Communications_Logs_Challenge2008** folder to an easily understandable, viewable, and readable rendering of the communications (remove non-conversation data). The supplied files were from either or both of the two computers used in the chat conversation. A detailed explanation of your process (software or technique) used to examine, extract, and present the data is required.

Points will be awarded for the completeness of the data recovered from the communications and the ease of understanding or utility of the method the information is reported from that file(s).

Total Weighted Points: 60 Total Points available per entry – Total 300 Points Available

1. **Answers** – Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law.*
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

Internal Reviewer Use Only

Reviewer:

Date:

Points Awarded:

Review Period: to

Completed: □ Yes □ No □ Partial

Question 302: Skype Chat

How to read other people's SKype chat: Youtube tutorial

http://www.youtube.com/watch?v=dt2GQjA1oWY

- Copy paste the Skype Folders

\Application\Skype

Select contents of user folder

Paste into your user Folder

Our process:

- setup your own Skype instance

- On a test workstation, download and install SKYPE.

- Register a "fake" user ID, provide a fake email address.

- Logon to Skype, make sure your account is valid

- Logoff Skype

- Go to folder 2_yogibear1953

- Copy all individual files from the folder (Just files, no folders)

- Go to your SKYPE folder

    - documents and settings> (username) > Application Data > Skype > (Username)

- Paste files from TARGET's Skype Folder (just the files, no folders)

- Log on to Skype

- Go to Contacts

- Click on suspect contacts name > Right-Click > view Chat History

Test Skype account: xxxxxxhead\(xxxxxxxxxxxx)

Suspect Users:

Blane Stallman (as himself)

kiki1932 (bob zeus)

Decoded Skype Messages:

```
{\rtf1\ansi\ansicpg1252\deff0\deflang1033{\fonttbl{\f0\fswiss\fcharset0 Arial;}}

{\*\generator Msftedit 5.41.15.1507;}\viewkind4\uc1\pard\f0\fs20 [3/5/2008 1:38:21 PM] Bob Zeus says: hey, it's me, you there?\par

[3/5/2008 1:39:01 PM] Blane Stallman says: yea, i'm here, what's up?\par

[3/5/2008 1:52:51 PM] Blane Stallman says: hold on, got an important phone call.  i'll get back with u\par

[3/5/2008 1:53:15 PM] Bob Zeus says: ok\par

[3/31/2008 10:54:59 AM] Blane Stallman says: So Bob, what's happening, you haven't been on in awhile?\par

[3/31/2008 10:55:24 AM] Bob Zeus says: Sorry, been taking care of all the other business herer, didn't have the time.\par

[3/31/2008 10:56:08 AM] Blane Stallman says: You know we still have that time thing going on, we miss our chance and we're out of luck this time, maybe for a long time\par

[3/31/2008 10:56:16 AM] Bob Zeus says: you know, we shouldn't be using names int htis converstion and yea I know about the time thing but we gotta be careful man\par

[3/31/2008 10:56:48 AM] Blane Stallman says: sorry didn't think about the name thing just nervous I guess\par

[3/31/2008 10:56:55 AM] Bob Zeus says: Jut think about what your going to do with all that money and youll feel better soon\par

[3/31/2008 10:57:00 AM] Blane Stallman says: Ok\par

[3/31/2008 10:57:07 AM] Bob Zeus says: you got the weapons and other gear?\par
```

also-ran

[3/31/2008 10:57:49 AM] Blane Stallman says: Yea, thought I was going to have a problem with the guns, by my uncle's a hunter and had a lot so I just "borrowed" some from him\par

[3/31/2008 10:57:58 AM] Bob Zeus says: Will he get wise?\par

[3/31/2008 10:58:40 AM] Blane Stallman says: Naw, he keps them in the basement and hasn't used them in years. they were in an old metal cabinet, dusty and dirty as all get out\par

[3/31/2008 10:58:48 AM] Bob Zeus says: Didn't leave any traces you were ther and took them out\par

[3/31/2008 10:59:31 AM] Blane Stallman says: Nope, used a rag over my nands and blew some dust back over where they had been sitting. Things were a pain to clean though\par

[3/31/2008 10:59:42 AM] Bob Zeus says: How bout the ammo?\par

[3/31/2008 10:59:57 AM] Blane Stallman says: I just went down and bought some new\par

[3/31/2008 11:00:09 AM] Bob Zeus says: Didn't have to give them a name or anything did you?\par

[3/31/2008 11:00:17 AM] Blane Stallman says: Nope, just like buying steaks at the grocery\par

[3/31/2008 11:00:20 AM] Bob Zeus says: Good, how bout the rest of the swtufff\par

[3/31/2008 11:01:01 AM] Blane Stallman says: Got an old can of black powder from his basement also, maybe 30 pounds, old but never been opened, should still be good\par

[3/31/2008 11:01:04 AM] Bob Zeus says: Didn't buy new\par

[3/31/2008 11:01:37 AM] Blane Stallman says: They would have wanted ID for that man, and I only have the one fake set and I didn't want to burn it on that\par

[3/31/2008 11:01:46 AM] Bob Zeus says: Good, whit what I got out of the anarchists cookbook combined with that were going to open some eyesw I'll tell you that\par

[3/31/2008 11:01:59 AM] Blane Stallman says: When we hit this place its going to be empty right?\par

[3/31/2008 11:02:48 AM] Bob Zeus says: Except for some roving security and I told you I scoped that out and timed them up. Always taking lunc together at the same time so we got an hour\par

[3/31/2008 11:02:49 AM] Blane Stallman says: I just don't want any mistakes. It's one thing to do this but murder, man they sick a needle in your arm and that stuff burning is the last thing you feel\par

[3/31/2008 11:03:28 AM] Bob Zeus says: Settle down. If we stick to the plan and do this right theyrll be no problems\par

[3/31/2008 11:03:31 AM] Blane Stallman says: Yea, that's what you say now, but that's not the way it worked out last time\par

[3/31/2008 11:04:13 AM] Bob Zeus says: That was justt bad luck, and it was bad luck for them. I didn't want anyone to get hurt, you know that\par

[3/31/2008 11:04:29 AM] Blane Stallman says: Don't change a thing man, you still killed them\par

[3/31/2008 11:04:56 AM] Bob Zeus says: Listen amigo you were right there too and unless you shut up and follwo the plan well both be looking a a ride on the needle SO SHUT YOUR MOUTH ABOUT THE LAST JOB\par

[3/31/2008 11:05:32 AM] Blane Stallman says: Don't talk to me that way. I've been loyal and haven't said a thing. I know they're still looking for who pulled that and that means us. I aint gonna help them kill me\par

[3/31/2008 11:05:40 AM] Bob Zeus says: Sorry, jut the pressure, I know you won't and didn't talk\par

\ul\b\i [3/31/2008 11:06:28 AM] Bob Zeus says: listen, we got this going and just need to chill awhile. Gotta get off this comm and get on the other one we set up so they cant trace us so good. Get up on that one, regular time and well finish the planning\ulnone\b0\i0\par

[3/31/2008 11:06:42 AM] Blane Stallman says: Ok man, later\par

[3/31/2008 11:06:48 AM] Bob Zeus says: later\par

}

0150-ren